SOME USES OF MICROCOMPUTERS IN NUMBER THEORY
RESEARCH

S. S. WAGSTAFF JR
Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, U.S.A.

Abstract—The development of number theory has been influenced greatly by the use of computers. Although many of these computers were comparatively large and fast when they were used, most of the work they did could have been done by modern microcomputers. This paper describes several ways microcomputers could have been used and can be used to aid research in number theory. Since this article updates a recent survey article of H. C. Williams on the influence of computers in the development of number theory, it discusses only a few problems such as factoring integers, testing integers for primality and Waring's problem.

1. INTRODUCTION

Seven years ago in this journal, Williams [1] surveyed some ways in which the development of number theory has been influenced by computers. He concludes by lamenting that his paper "will very soon be out of date". Indeed there have been several major breakthroughs during the past seven years in the problems he discussed. We will attempt here to update his paper and mention a few other ways computers have aided the development of number theory.

Nearly all of the computations Williams mentions could have been done by a microcomputer. Hence this article is appropriate for this issue. Here are the only three which have been pushed so far with large computers that they cannot be attacked with profit using microcomputers:

Fermat's "last theorem" is the conjecture that there are no non-zero integers, x, y, z and n > 2 with x^n + y^n = z^n. Using many hours on a Cyber 205, Tanner and I [2] have proved that this conjecture holds for all n < 150,000. The calculations are ideally suited for vector processors and not for microcomputers.

The largest known prime in mid-1988 is 2^{216091} - 1. It was just found by Slowinski in many minutes of Cray X-MP time. (See Ref. [3].) It would take thousands of hours for a microcomputer to test the primality of even a single M_p = 2^p - 1 for p near 216091.

van de Lune et al. [4] have verified the Riemann hypothesis for the first 1.5 \cdot 10^9 zeros of the Riemann zeta function \zeta(s): they all have real part \frac{1}{2}. Their result took more than a thousand hours on modern supercomputers. It will not be extended significantly with a micro.

This paper is not as long as it might have been because Williams [1] has recently said a great deal about this subject in this journal. Some terminology and notation [such as "Carmichael number" and \mu(n)] which are not explained below are defined in Ref. [1]. The use of computers in number theory research is so extensive that this paper also will very soon be out of date.

2. FACTORING

Writing in 1981, Williams [1] reported that any composite number of up to 46 digits can be routinely factored. That is where the Cunningham project stood then. The goal of the Cunningham project is to factor numbers b^n \pm 1 for small b. During the past half century researchers have extended the work of Cunningham [5]. In 1983, Brillhart et al. published a book [6] which updates Ref. [5]. Appendix C of Ref. [6] lists some composite divisors of b^n \pm 1 whose factorization is still sought. It gives 10–20 composite numbers of d digits for each d in a large range. Versions of this Appendix have been maintained for many years by the authors of Ref. [6]. A copy of it which resides in a data set at Purdue University changes frequently as people factor some of the numbers. The smallest number in the snapshot of Appendix C published in 1983 had 51 digits. In 1981 the Appendix had 47 digits. In 1985 it had 54 digits. In early 1987 it had 76 digits. In mid-1988 it had 83 digits. This number of digits is a crude measure of our ability to factor integers.
Another bench mark of factoring techniques is the "ten most wanted list" of the Cunningham project. The version [6] of it published in 1983 contained numbers of 53–71 digits. All ten of them were factored in 1983 and 1984 by Davis and Holdridge [7] using a Cray-1 and a Cray X-MP. (Two of these were factored independently by others.) Several new "ten most wanted lists" were then formulated and many of their entries factored. In 1987 the numbers on the list had between 87 and 148 digits.

How were these achievements made possible? The increase in size from 47 to 83 digits in the least entry of the Cunningham Appendix C required the factorization of hundreds of large integers. Many of these factorizations could have been done by microcomputers. Some of them were done by microcomputers. Many of them were done in 1982 and 1983 by an improvement of the Morrison–Brillhart [8] continued fraction algorithm (CFRAC). In the heart of CFRAC one divides many numbers $Q_k$ by a small set of primes $F = \{q_i\}_{i = 1, 2, \ldots, s}$ called the factor base. The only $Q_k$ which are useful are those which can be factored completely using the primes in $F$. Morrison and Brillhart [8] and others suggested that one should pause part way through the factor base during the trial division for $Q_k$ and, if the remaining cofactor was too large, abandon $Q_k$ and proceed to $Q_{k+1}$. Pomerance [9] analyzed and promoted this early abort strategy (EAS). He predicted how far through $F$ one should pause, what size cofactor was too large to continue and how much acceleration one would achieve. He and I [10] factored many numbers and experimented with the parameters to find good practical choices for them. By using several early aborts we were able to factor 54-digit numbers in less time than it took to factor 47-digit numbers using CFRAC without EAS. Now microcomputers can factor hard 40-digit numbers by CFRAC in a few days.

Another factoring algorithm, the quadratic sieve method (QS), was invented in 1981. Let $N$ be the number to factor. (We follow Williams' [1] notation.) Put

$$m = \lceil \sqrt{N} \rceil$$

(the largest integer less than $\sqrt{N}$) and

$$r_k = (m + k)^2 - N = m^2 - N + 2km + k^2.$$  

Pomerance [9] noticed that one may factor the $r_k$ with a sieve like the one Schroeppe1 used (it was mentioned in Ref. [1]): If $k_1$ and $k_2$ are the two solutions of the congruence $(m + k)^2 - N \equiv 0 \pmod{q_i}$, then the values of $k$ for which $q_i$ divides $r_k$ are exactly the $k$ in the union of the two arithmetic progressions $k_1 + jq_i$, $k_2 + jq_i$, $j$ an integer. This technique avoids the trial division which is the slowest part of CFRAC. Davis and Holdridge [7] used QS to factor the "ten most wanted" numbers. QS is about as fast as CFRAC with EAS for factoring numbers up to 20–30 digits. QS is faster than CFRAC for larger numbers. Davis and Holdridge factored the 71-digit number $(10^{71} - 1)/9$ in a few hours of Cray X-MP time.

In 1985 Peter Montgomery found a way to choose many other quadratic polynomials to "fit" $N$ and the length of the sieve interval. Silverman [11] implemented Montgomery's ideas, called the multiple polynomial quadratic sieve, on a VAX and then on a network of SUN microcomputers. His program, running on about a dozen micros, was for several years the champion for factoring large integers. His two programs factored most of the Cunningham numbers of 54–82 digits. A large number of microcomputers connected by a network would appear to be an ideal machine for factoring numbers by the QS method. Another excellent device for factoring is the NEC SX/2 supercomputer. It was used by te Riele in May 1988, to factor a 92-digit number and set a new record for largest number factored by the QS algorithm.

Now that factoring has become such a popular endeavor, new algorithms for it are being invented about once a year. Schnorr and Lenstra Jr [12] invented a Monte Carlo method (CPS) which uses class numbers of quadratic fields. Coppersmith et al. [13] created the residue list sieve algorithm which has theoretical interest but which is probably not practical. Another new algorithm is the cubic sieve [13, 14], which may be practical.

Lenstra Jr has invented a new factoring method which uses elliptic curves. Assuming certain reasonable hypotheses, all methods mentioned above can factor $N$ in time $\exp((c + o(1))\sqrt{\log N \log \log N})$ operations for various constants $c$. Lenstra's elliptic curve method (ECM) will discover the prime factor $p$ of $N$ in $\exp((1 + o(1))\sqrt{2 \log p \log \log p})$ operations. It usually discovers small factors more quickly than large ones and, even in the worst case when $p$ is near $\sqrt{N}$, the method is not worse than the above methods. It requires little memory and is
suitable for programming on a microcomputer. Montgomery and Silverman have already factored many of the new "wanted" Cunningham numbers with ECM. They each have factored hundreds of numbers from Ref. [5] with this method. Brent has factored several Mersenne numbers on a microvax with ECM. Lenstra and Manasse have factored several "wanted" numbers from the Cunningham project by running ECM on hundreds of microcomputers at DEC. A large number of microcomputers connected by a network would appear to be an ideal machine for factoring numbers by ECM.

Smith and I [15] have built a special processor, the extended precision operand computer (EPOC), to factor numbers with CFRAC. This machine has a 128 bit word length and several remaining units to perform trail division swiftly. The hardware was designed to fit the inner loop of the CFRAC algorithm. It uses a microcomputer as a host computer. The EPOC systems programs and data preparation programs run on the microcomputer. The EPOC is not the first machine whose design was influenced by requirements of number theory algorithms. Lehmer [16–19] has built several devices for solving congruences by sieving. Many factorizations and primality tests were done using his sieves. Rudd et al. [20] are building a special processor for factoring by the CPS method. At the University of Georgia, Pomerance et al. [21] are building a machine for QS.

We conclude this section on factoring with a practical application of factoring: Sometimes algebraic identities can be discovered by study of a table of factored numbers. Here is an excerpt from a table of numbers $2n + 1$ factored into primes:

<table>
<thead>
<tr>
<th>$n$</th>
<th>Prime factorization of $2^n + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>$5 \cdot 13$</td>
</tr>
<tr>
<td>10</td>
<td>$5^2 \cdot 41$</td>
</tr>
<tr>
<td>14</td>
<td>$5 \cdot 29 \cdot 113$</td>
</tr>
</tbody>
</table>

5 divides each of these numbers because $x^2 + 1$ divides $x^{2h} + 1$ when $h$ is odd. However, we are looking for something deeper than cyclotomic factorizations here. Write the factorizations as:

<table>
<thead>
<tr>
<th>$n$</th>
<th>Factorization of $2^n + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$1 \cdot 5$</td>
</tr>
<tr>
<td>6</td>
<td>$5 \cdot 13$</td>
</tr>
<tr>
<td>10</td>
<td>$25 \cdot 41$</td>
</tr>
<tr>
<td>14</td>
<td>$113 \cdot 145$</td>
</tr>
</tbody>
</table>

and one sees that the factors are:

<table>
<thead>
<tr>
<th>$n$</th>
<th>Factorization of $2^n + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$(2^2 - 2^1 + 1)(2^2 + 2^1)$</td>
</tr>
<tr>
<td>6</td>
<td>$(2^2 - 2^1 + 1)(2^2 + 2^1)$</td>
</tr>
<tr>
<td>10</td>
<td>$(2^5 - 2^3 + 1)(2^5 + 2^3)$</td>
</tr>
<tr>
<td>14</td>
<td>$(2^7 - 2^4 + 1)(2^7 + 2^4)$</td>
</tr>
</tbody>
</table>

This suggests that in general

$$2^{2h} + 1 = (2^h - 2^k + 1)(2^h + 2^k + 1),$$

where $h = 2k - 1$. This identity is easy to prove once it has been noticed. The identity gives an affirmative answer to this question: for each $k$ does there exist an integer with exactly $k$ one bits in its binary representation which can be multiplied by an integer with three one bits to give a product with only two one bits? The identity also provides a useful trick to ease the task of factoring numbers of the form $2^{2h} + 1$. (See Knuth [22, Section 4.5.4.]) Aurifeuille (see Ref. [23, p. 383]) discovered this identity and others with 2 replaced by different bases. For example, the base 3 identity is

$$3^{2h} + 1 = (3^h - 3^k + 1)(3^h + 3^k + 1), \quad h = 2k - 1.$$  

(Of course, $3^{2h} + 1 = (3^h + 1)(3^{2h} - 3^h + 1)$ for all $h$ and $x^2 - x + 1$ is irreducible. What Aurifeuille found was that the trinomial factor could be factored algebraically whenever $h$ is odd.)

Cunningham worked out these identities up to base 12 by hand. Recently, Silverman has computed them up to about base 30 using VAXIMA. No doubt they could be computed up to at
least base 100 on a microcomputer. Stevenhagen [24] gives an efficient method for computing them via the Euclidean algorithm.

Do there exist other, undiscovered identities like those of Aurifeuille? I think so.

3. PRIMALITY TESTING

Since 1982, Slowinski has found three more Mersenne primes, namely, $M_p$ for $p = 86243, 132049$ and 216091. (See Ref. [3].) The interval $p \leq 216091$ has not been searched completely, but Haworth has searched exhaustively up to 100000. In 1988, Colquitt and Welsch found a Mersenne prime, $M_{10903}$, which Slowinski overlooked. Although, as I said in the introduction, microcomputers cannot be used to test such large $M_p$ for primality, they can be used in another way in the search for large Mersenne primes. About half of the Mersenne numbers $M_p$ with $10^5 < p < 10^6$ have a prime divisor small enough for a microcomputer to find in a short time. Microcomputers can be used to weed out many composite $M_p$, probably more cheaply than having a supercomputer perform a preliminary search for these small prime factors.

Cohen and Lenstra Jr [25] have improved the new primality testing algorithm of Adleman et al. [26]. The improvements avoid evaluating the mock residue symbols and accelerate the algorithm. While the number of elementary operations needed to test $N$ for primality remains $O((\log N)^\delta \log \log N)$, the improved test requires less than a minute on a large computer for a 100-digit number and only a few minutes for a 200-digit prime. Several thousand prime and probable prime divisors of numbers of the form $b^n \pm 1$ are listed in Appendix A of the Cunningham project [6]. When that book was published in 1983, primality proofs had been completed for all numbers in Appendix A up to about 60 digits. (Some larger ones had been done, too.) In 1984, Lenstra and Odlyzko proved primality of these numbers up to about 210 digits. A microcomputer should be able to prove the primality of any prime up to 100 digits by these methods. Cohen and Lenstra [27] discuss the implementation of this new algorithm. In 1988, Morain programmed a primality testing algorithm which uses elliptic curves and used it to complete the proofs of primality of all the probable primes remaining in Appendix A of Ref. [6].

In 1986, Williams and Dubner [28] proved that the repunit $(10^{1001} - 1)/9$ is prime. This number was known for years to be probably prime.

A few years ago, the record for largest known Carmichael number was held by Woods and Huenemann [29]. They remarked when presenting their 432-digit example that they probably would hold this record for a very short time. Later, Atkin and Dubner each held the record for a while. Recently, Löh found one with more than 10000 digits—and he is still looking for larger ones.

Merten's function is the summatory function of the Möbius function:

$$M(x) = \sum_{n=1}^{x} \mu(n).$$

Williams [1] reported that Neubauer used a computer to disprove von Sterneck's conjecture that $|M(x)| < \frac{1}{2} \sqrt{x}$, for all $x > 200$. Another conjecture about $M(x)$ is Merten's conjecture that $|M(x)| \leq \sqrt{x}$, for all $x$. The truth of this conjecture has been verified for all $x \leq 10^8$. However, Odlyzko and te Riele [30] disproved Mertens' conjecture in 1985. It fails for some $x < 10^{10^6}$, but they did not exhibit an $x$ with $|M(x)| > \sqrt{x}$.

4. OTHER TOPICS

In recent issues of the Mathematical Intelligencer, Stan Wagon has written an informative column called "The Evidence". This series of articles explores the reasons why some mathematicians believe various conjectures. One source of such evidence is computers. For example, he discusses [31] why we think $\pi$ is normal, that is, why we think its digits occur with equal frequency in any base.
In 1981, Bohman and Fröberg [32] wrote a significant new chapter on Waring’s problem for cubes. Wieferich had proved that every positive integer can be expressed as the sum of at most 9 cubes of positive integers. Landau proved that 8 cubes are enough to represent all sufficiently large integers. (Only 23 and 239 need 9 cubes.) Linnik [33] showed that 7 cubes will do for all sufficiently large integers and Watson [34] gave a simple proof of this fact. It is easy to prove that infinitely many integers require at least 4 cubes. The problem is to find the smallest number $G$ of cubes which are needed to represent all sufficiently large integers. We have $4 \leq G \leq 7$ from what was just said. Hand calculations before the age of electronic computers suggested that 454 and 8042 were the largest integers requiring 8 and 7 cubes, respectively. A few numbers near the limit (about $10^9$) of these calculations continued to require 6 cubes and many needed 5 cubes.

Bohman and Fröberg [32] used a computer to extend the hand calculations. Their results suggest that 1,290,740 is the largest integer which needs 6 cubes. They sampled intervals up to $4 \cdot 10^{11}$ and graphed the results. The graph suggests that $G = 4$ and that all integers $> 10^{13}$ require no more than 4 cubes.

Roth [35] proved that if $x$ is an irrational algebraic number and $\epsilon > 0$, then there are only finitely many pairs of integers $q > 0, h$ such that $|qx - h| < 1/q^{1+\epsilon}$. Lang and Trotter [36] computed and studied the continued fraction expansions of several simple algebraic numbers (such as cube roots of integers). The rational approximations $h/q$ which they found to these numbers were never as close as one might expect from Roth’s theorem. They concluded that it may be possible to improve Roth’s theorem in the form that if $x$ is an irrational algebraic number and $\epsilon > 0$, then there are only finitely many pairs of integers $q > 0, h$ such that $|qx - h| < 1/(qf(q))$, where $f(q)$ is a function “close” to the logarithm, such as $(\log q)^{1+\epsilon}$ or $c \log q$.

When $S$ is a set of integers and $n$ is a positive integer write $S(n)$ for the number of positive integers $\leq n$ in $S$. The asymptotic density of $S$ is $d(S) = \lim_{n \to \infty} S(n)/n$ if the limit exists. The Schnirelmann density of $S$ is $\sigma(S) = \inf S(n)/n$, where the infimum is over positive integers $n$. Sometimes $\sigma(S) = d(S)$, as when $S$ is the set of all odd integers, and sometimes $\sigma(S) < d(S)$, as when $S$ is the set of all even integers. A less trivial example is the set $S$ of squarefree integers (those not divisible by a square greater than 1) which has $d(S) = 6/\pi^2$ and $\sigma(S) = 53/88$. (See Ref. [37]. The infimum is attained at $n = 176$.)

It is known that a positive integer can be expressed as the sum of three squares of integers if and only if it is not of the form $4^a(8b + 7)$, where $a$ and $b$ are non-negative integers. The first few integers which are not the sum of three squares are 7, 15, 23, 28, 31, ... Let $S$ be the set of integers which are the sum of three squares. It is easy to prove that $d(S) = 5/6$. The statement $\sigma(S) = 5/6$ is equivalent to $S(n) = 5n/6$, for all $n$. A short calculation shows that the inequality holds for the first few hundred $n$. If one tries to prove it for all $n$ by induction, one finds that the induction hypothesis is too weak to yield the desired conclusion. But the calculation actually reveals that $S(n) > (5n + 1)/6$. This induction hypothesis is just what is needed to prove that $\sigma(S) = 5/6$. My paper [38] proving this fact does not mention computing at all because it was not needed in the end. Shiu [39] gives a fresh approach to this problem.

Occasionally, the easy availability of computers can cause one to overlook simple theoretical solutions to problems. Several years ago I needed the approximate numerical value of the infinite product

$$
\prod_{\text{prime } p} \frac{p^2 + 1}{p^2 - 1}.
$$

There was a computer terminal at hand. I wrote a short program to generate the primes $\leq x$ with a sieve and compute the partial product for these primes. In a few moments this table appeared on my terminal:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\pi(x)$</th>
<th>Partial product up to $x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4</td>
<td>2.350984</td>
</tr>
<tr>
<td>100</td>
<td>25</td>
<td>2.490394</td>
</tr>
<tr>
<td>1000</td>
<td>168</td>
<td>2.499360</td>
</tr>
<tr>
<td>10000</td>
<td>1229</td>
<td>2.499851</td>
</tr>
<tr>
<td>100000</td>
<td>9592</td>
<td>2.499996</td>
</tr>
</tbody>
</table>
Based on this evidence, I conjectured that the infinite product exactly equals \(5/2\), and, after a few minutes, found this proof:

\[
\prod_{\text{prime } p} \frac{p^2 + 1}{p^2 - 1} = \prod_{\text{prime } p} \frac{1 - p^{-4}}{(1 - p^{-2})^2} = \frac{\pi^4}{90} \left(\frac{\zeta(4)}{\zeta^2(2)}\right) = \left\lfloor \frac{\pi^4}{6} \right\rfloor = 5 - \frac{1}{2}.
\]

Later I learned that Euler had given the same proof.

Acknowledgement—Research partially supported by National Science Foundation Grant DCR-8603449.

REFERENCES

5. A. J. C. Cunningham and H. J. Woodall, *Factorization of \(y^a \pm 1\), \(y = 2, 3, 5, 6, 7, 10, 11, 12\) Up to High Powers (n)*, Hodgson, London (1925).